

Loop Calculus Helps to Improve Belief Propagation and Linear Programming Decodings of Low-Density-Parity-Check Codes

Michael Chertkov¹ & Vladimir Chernyak ^{2,1}

¹CNLS & T-13, LANL and ²Wayne State, Detroit

Allerton, 09/27/06

Thanks to M. Stepanov (UofA, Tucson)

Outline

1 Introduction

- Error Correction, LDPC
- Statistical Inference, Graphical Models
- Bethe free energy, LP decoding
- Error-Floor, Pseudo-codewords & Instantons

2 Pseudo-Codeword Search Algorithm

3 Loop Calculus

- Loop Series for Partition function
- Derivation Sketch
- Loop calculus helps to analyze pseudo-codewords

4 Effective Free Energy Approach

- Extended Variational Principle & Loop-Corrected BP
- LP-Erasure Algorithm

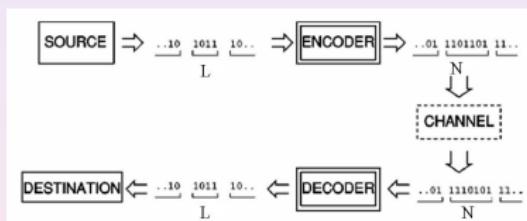
5 Conclusions

- Results
- Path Forward
- Bibliography

Error Correction



Scheme:



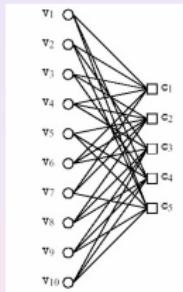
Example of Additive White Gaussian Channel:

$$P(\mathbf{x}_{out} | \mathbf{x}_{in}) = \prod_{i=bits} p(x_{out;i} | x_{in;i})$$

$$p(x|y) \sim \exp(-s^2(x - y)^2 / 2)$$

- **Channel**
is noisy "black box" with only statistical information available
- **Encoding:**
use redundancy to redistribute damaging effect of the noise
- **Decoding:**
reconstruct most probable codeword by noisy (polluted) channel

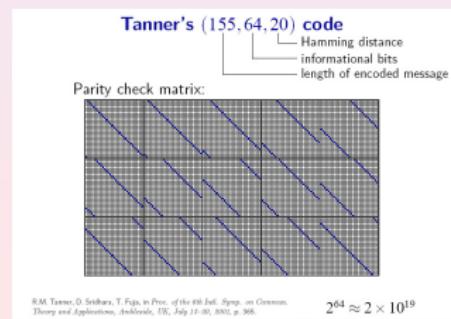
Low Density Parity Check Codes



- N bits, M checks, $L = N - M$ information bits
example: $N = 10, M = 5, L = 5$
- 2^L codewords of 2^N possible patterns
- Parity check: $\hat{H}\mathbf{v} = \mathbf{c} = \mathbf{0}$
example:

$$\hat{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

- LDPC = graph (parity check matrix) is sparse



Maximum Likelihood/Maximum-a-Posteriori

Exhaustive search for pre-image = the best one can possibly do

$$\text{ML} = \arg \max_{\sigma=\text{codewords}} P(\mathbf{x}_{\text{out}}|\sigma); \quad \text{MAP} = \left| \frac{\sum_{\sigma} \sigma P(\mathbf{x}_{\text{out}}|\sigma)}{\sum_{\sigma} P(\mathbf{x}_{\text{out}}|\sigma)} \right|$$

MAP≈BP=Belief-Propagation (Bethe-Pieirls)

Gallager '61

- Exact on a tree
- Trading optimality for reduction in complexity: $\sim 2^L \rightarrow \sim L$
- BP = solving equations on the graph:

$$\eta_{j\alpha} = h_j + \sum_{\substack{j \in \beta \\ \beta \neq \alpha}} \tanh^{-1} \left(\prod_{\substack{i \in \beta \\ i \neq j}} \tanh \eta_{i\beta} \right)$$

- Message Passing = iterative BP
- Applies to a general inference problem on a (sparse) graph

Maximum Likelihood/Maximum-a-Posteriori

Exhaustive search for pre-image = the best one can possibly do

$$\text{ML} = \arg \max_{\sigma=\text{codewords}} P(\mathbf{x}_{\text{out}}|\sigma); \quad \text{MAP} = \left| \frac{\sum_{\sigma} \sigma P(\mathbf{x}_{\text{out}}|\sigma)}{\sum_{\sigma} P(\mathbf{x}_{\text{out}}|\sigma)} \right|$$

MAP≈BP=Belief-Propagation (Bethe-Pieirls)

Gallager '61

- Exact on a tree
- Trading **optimality** for reduction in complexity: $\sim 2^L \rightarrow \sim L$
- BP = solving equations on the graph:

$$\eta_{j\alpha} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \in \beta, i \neq j} \tanh \eta_{i\beta} \right)$$

- Message Passing = iterative BP
- Applies to a **general inference** problem on a (sparse) graph

Graphical models of Statistical Inference

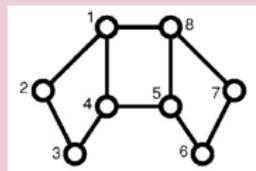
Factorization

(Forney '01, Loeliger '01)

$$P\{\boldsymbol{\sigma}\} = \prod_{a \in X} f_a(\boldsymbol{\sigma}_a),$$

$$Z = \sum_{\{\boldsymbol{\sigma}\}} P\{\boldsymbol{\sigma}\},$$

X = edges



$$f_a \geq 0$$

$$\sigma_{ab} = \sigma_{ba} = \pm 1$$

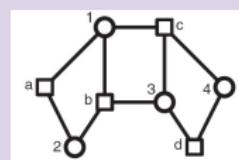
$$\boldsymbol{\sigma}_1 = (\sigma_{12}, \sigma_{14}, \sigma_{18})$$

$$\boldsymbol{\sigma}_2 = (\sigma_{12}, \sigma_{13})$$

Error-Correction (bipartite)

$$f_i(\boldsymbol{\sigma}_i) = \begin{cases} 1, & \sigma_{i\alpha} = \sigma_{i\beta} \\ 0, & \text{otherwise} \end{cases}$$

$$f_\alpha(\boldsymbol{\sigma}_\alpha) = \delta \left(\prod_{i \in \alpha} \sigma_i, +1 \right) \exp \left(\sum_{i \in \alpha} \sigma_i h_i / q_i \right)$$



h_i - log-likelihoods
 q_i -connectivity degrees

Bethe free energy: variational approach

(Yedidia,Freeman,Weiss '01 -

inspired by Bethe '35, Peierls '36)

$$F = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a) + \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln b_a(\sigma_a) - \sum_{(a,c)} b_{ac}(\sigma_{ac}) \ln b_{ac}(\sigma_{ac})$$

constraints:

$$\forall a, c; c \in a : 0 \leq b_a(\sigma_a), b_{ac}(\sigma_{a,c}) \leq 1$$

$$\forall a, c; c \in a : \sum_{\sigma_a} b_a(\sigma_a) = \sum_{\sigma_{a,c}} b_{ac}(\sigma_{a,c}) = 1$$

$$\forall a; c \in a : b_{ac}(\sigma_{ac}) = \sum_{\sigma_a \setminus \sigma_{ac}} b_a(\sigma_a)$$

Belief-Propagation Equations:

$$\frac{\delta F}{\delta b} \Big|_{\text{constr.}} = 0$$

- Convergence of iterative BP is not guaranteed

- Relaxation to minimum of the Bethe Free energy enforces convergence of iterative BP (Stepanov, Chertkov '06)

LP decoding

Feldman, Wainwright, Karger '03

- LP decoding = minimization of a linear function over a bounded domain described by linear conditions
- Fast and Discrete
- "Large SNR" limit of BP:

$$F \approx E = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a)$$

Bethe free energy: variational approach

(Yedidia,Freeman,Weiss '01 -

inspired by Bethe '35, Peierls '36)

$$F = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a) + \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln b_a(\sigma_a) - \sum_{(a,c)} b_{ac}(\sigma_{ac}) \ln b_{ac}(\sigma_{ac})$$

constraints:

$$\forall a, c; c \in a : 0 \leq b_a(\sigma_a), b_{ac}(\sigma_{a,c}) \leq 1$$

$$\forall a, c; c \in a : \sum_{\sigma_a} b_a(\sigma_a) = \sum_{\sigma_{a,c}} b_{ac}(\sigma_{a,c}) = 1$$

$$\forall a; c \in a : b_{ac}(\sigma_{ac}) = \sum_{\sigma_a \setminus \sigma_{ac}} b_a(\sigma_a)$$

Belief-Propagation Equations:

$$\frac{\delta F}{\delta b} \Big|_{\text{constr.}} = 0$$

- Convergence of iterative BP is not guaranteed

- Relaxation to minimum of the Bethe Free energy enforces convergence of iterative BP (Stepanov, Chertkov '06)

LP decoding

Feldman, Wainwright, Karger '03

- LP decoding = minimization of a linear function over a bounded domain described by linear conditions
- Fast and Discrete
- "Large SNR" limit of BP:

$$F \approx E = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a)$$

Bethe free energy: variational approach

(Yedidia,Freeman,Weiss '01 -

inspired by Bethe '35, Peierls '36)

$$F = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a) + \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln b_a(\sigma_a) - \sum_{(a,c)} b_{ac}(\sigma_{ac}) \ln b_{ac}(\sigma_{ac})$$

constraints:

$$\forall a, c; c \in a : 0 \leq b_a(\sigma_a), b_{ac}(\sigma_{a,c}) \leq 1$$

$$\forall a, c; c \in a : \sum_{\sigma_a} b_a(\sigma_a) = \sum_{\sigma_{a,c}} b_{ac}(\sigma_{a,c}) = 1$$

$$\forall a; c \in a : b_{ac}(\sigma_{ac}) = \sum_{\sigma_a \setminus \sigma_{ac}} b_a(\sigma_a)$$

Belief-Propagation Equations:

$$\frac{\delta F}{\delta b} \Big|_{\text{constr.}} = 0$$

- Convergence of iterative BP is not guaranteed

- Relaxation to minimum of the Bethe Free energy enforces convergence of iterative BP (Stepanov, Chertkov '06)

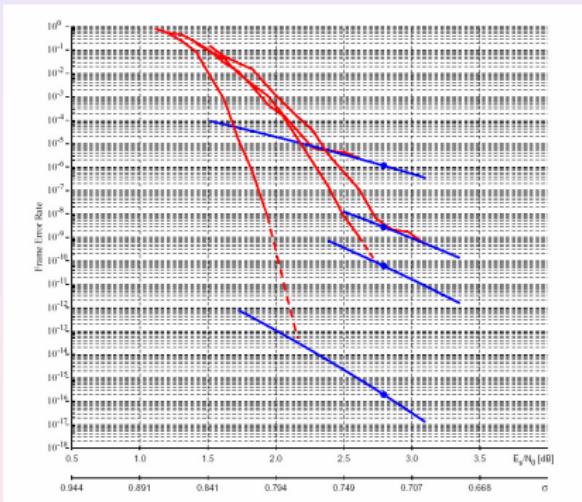
LP decoding

Feldman, Wainwright, Karger '03

- LP decoding = minimization of a linear function over a bounded domain described by linear conditions
- Fast and Discrete
- "Large SNR" limit of BP:

$$F \approx E = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a)$$

Error-Floor



T. Richardson, Allerton '03

- BER vs SNR = measure of performance
- Waterfall \leftrightarrow Error-floor
- Suboptimal decoding causes error-floor:** at $E_s/N_0 \rightarrow \infty$,
 $FER_{ML} \sim \exp(-d_{ML}E_s/N_0)$ vs
 $FER_{sub} \sim \exp(-d_{sub}E_s/N_0)$ where
 $d_{ML} > d_{sub}$
- Monte-Carlo is useless at $BER \lesssim 10^{-8}$

Pseudo-codewords and Instantons

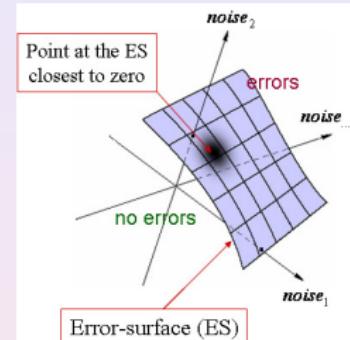
Error-floor is caused by (rare) troublemakers

instantons → pseudo-codewords

log-likelihoods → a-posteriori log-likelihoods

Bibliography:

- Pseudo-codewords & Error-floor:
 Wiberg '96; Forney et.al'99; Frey et.al '01;
 Richardson '04; Vontobel, Koetter '04-'06
- Instantons:
 Stepanov et.al '04-'06



Shopping list

- Analyze the troublemakers
- Improve decoding to reduce the error-floor

Pseudo-codewords and Instantons

Error-floor is caused by (rare) troublemakers

instantons → pseudo-codewords

log-likelihoods → a-posteriori log-likelihoods

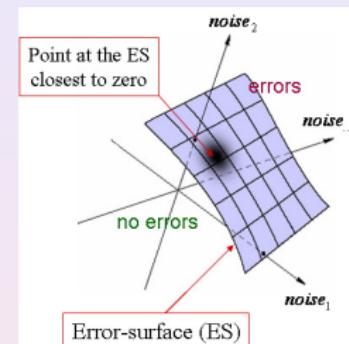
Bibliography:

- Pseudo-codewords & Error-floor:

Wiberg '96; Forney et.al'99; Frey et.al '01;
 Richardson '04; Vontobel, Koetter '04-'06

- Instantons:

Stepanov et.al '04-'06



Shopping list

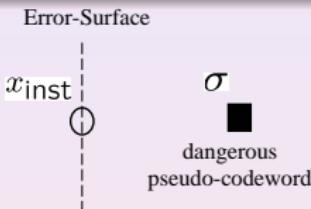
- Analyze the troublemakers
- Improve decoding to reduce the error-floor

LP decoding

$(\sigma_i = 0, 1 \quad \text{AWGN channel})$

Minimize, $E = \sum_{\alpha} \sum_{\sigma_{\alpha}} b_{\alpha}(\sigma_{\alpha}) \sum_{i \in \alpha} \sigma_i (1 - 2x_i) / q_i$, under $0 \leq b_i(\sigma_i)$, $b_{\alpha}(\sigma_{\alpha}) \leq 1$

$$\forall \alpha : \sum_{\sigma_{\alpha}} b_{\alpha}(\sigma_{\alpha}) = 1, \quad \& \quad \forall i \forall \alpha \exists i : b_i(\sigma_i) = \sum_{\sigma_{\alpha} \setminus \sigma_i} b_{\alpha}(\sigma_{\alpha})$$



Conditioned Median:

$$x_{\text{inst}} = \frac{\sigma}{2} \frac{\sum_i \sigma_i}{\sum_i \sigma_i^2}, \quad d = \frac{(\sum_i \sigma_i)^2}{\sum_i \sigma_i^2}$$

$$\text{FER} \sim \exp(-d \cdot s^2/2)$$

Wiberg '96; Forney et.al '01
Vontobel, Koetter '03,'05

Pseudo-Codeword-Search Algorithm

Chertkov, Stepanov '06

- Start: Initiate $x^{(0)}$.
- Step 1: $x^{(k)}$ is decoded to $\sigma^{(k)}$.
- Step 2: Find $y^{(k)}$ – conditioned median between $\sigma^{(k)}$, and "0"
- Step 3: If $y^{(k)} = y^{(k-1)}$, $k_* = k$ End.
Otherwise go to Step 2 with
 $x^{(k+1)} = y^{(k)} + 0$.

(155, 64, 20), AWGN test:

- Fast Convergence

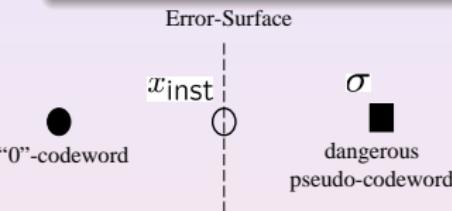


~ 200 pseudo-codewords within
 $16.4037 < d < 20$

LP decoding $(\sigma_i = 0, 1 \text{ AWGN channel})$

Minimize, $E = \sum_{\alpha} \sum_{\sigma_{\alpha}} b_{\alpha}(\sigma_{\alpha}) \sum_{i \in \alpha} \sigma_i (1 - 2x_i) / q_i$, under $0 \leq b_i(\sigma_i), b_{\alpha}(\sigma_{\alpha}) \leq 1$

$$\forall \alpha : \sum_{\sigma_{\alpha}} b_{\alpha}(\sigma_{\alpha}) = 1, \quad \& \quad \forall i \forall \alpha \ni i : b_i(\sigma_i) = \sum_{\sigma_{\alpha} \setminus \sigma_i} b_{\alpha}(\sigma_{\alpha})$$



Conditioned Median:

$$x_{\text{inst}} = \frac{\sigma}{2} \frac{\sum_i \sigma_i}{\sum_i \sigma_i^2}, \quad d = \frac{(\sum_i \sigma_i)^2}{\sum_i \sigma_i^2}$$

$$\text{FER} \sim \exp(-d \cdot s^2/2)$$

Wiberg '96; Forney et.al '01
Vontobel, Koetter '03,'05

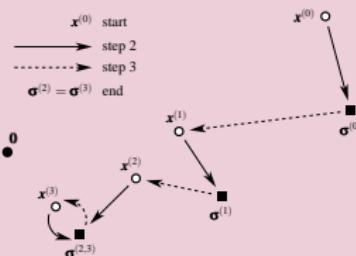
(155, 64, 20), AWGN test:

- Fast Convergence



Pseudo-Codeword-Search Algorithm

Chertkov, Stepanov '06



- Start: Initiate $x^{(0)}$.
- Step 1: $x^{(k)}$ is decoded to $\sigma^{(k)}$.
- Step 2: Find $y^{(k)}$ - conditioned median between $\sigma^{(k)}$, and "0"
- Step 3: If $y^{(k)} = y^{(k-1)}$, $k_* = k$ End.
Otherwise go to Step 2 with
 $x^{(k+1)} = y^{(k)} + 0$.

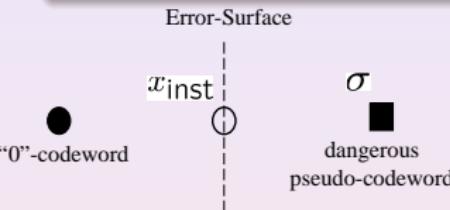
~ 200 pseudo-codewords within
 $16.4037 < d < 20$

LP decoding

$(\sigma_i = 0, 1 \text{ AWGN channel})$

Minimize, $E = \sum_{\alpha} \sum_{\sigma_{\alpha}} b_{\alpha}(\sigma_{\alpha}) \sum_{i \in \alpha} \sigma_i (1 - 2x_i) / q_i$, under $0 \leq b_i(\sigma_i)$, $b_{\alpha}(\sigma_{\alpha}) \leq 1$

$$\forall \alpha : \sum_{\sigma_{\alpha}} b_{\alpha}(\sigma_{\alpha}) = 1, \quad \& \quad \forall i \forall \alpha \ni i : b_i(\sigma_i) = \sum_{\sigma_{\alpha} \setminus \sigma_i} b_{\alpha}(\sigma_{\alpha})$$



Conditioned Median:

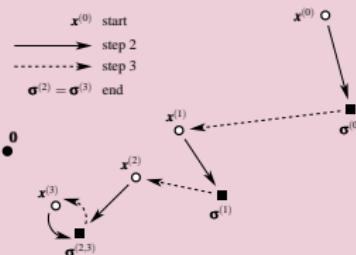
$$x_{\text{inst}} = \frac{\sigma}{2} \frac{\sum_i \sigma_i}{\sum_i \sigma_i^2}, \quad d = \frac{(\sum_i \sigma_i)^2}{\sum_i \sigma_i^2}$$

$$\text{FER} \sim \exp(-d \cdot s^2/2)$$

Wiberg '96; Forney et.al '01
Vontobel, Koetter '03,'05

Pseudo-Codeword-Search Algorithm

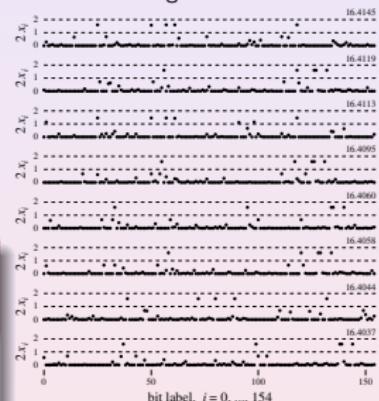
Chertkov, Stepanov '06



- **Start:** Initiate $x^{(0)}$.
- **Step 1:** $x^{(k)}$ is decoded to $\sigma^{(k)}$.
- **Step 2:** Find $y^{(k)}$ - conditioned median between $\sigma^{(k)}$, and "0"
- **Step 3:** If $y^{(k)} = y^{(k-1)}$, $k_* = k$ End.
Otherwise go to Step 2 with
 $x^{(k+1)} = y^{(k)} + 0$.

(155, 64, 20), AWGN test:

- Fast Convergence



~ 200 pseudo-codewords within
 $16.4037 < d < 20$

Loop Calculus:

(Chertkov, Chernyak '06)

Exact expression (for partition function, etc)
 in terms of BP

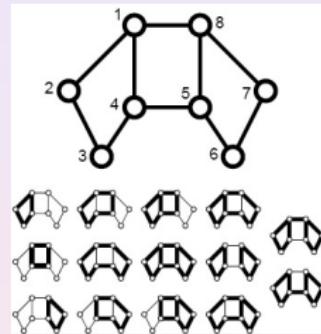
$$Z = Z_0 \left(1 + \sum_C r(C) \right), \quad r(C) = \frac{\prod_{a \in C} \mu_a}{\prod_{(ab) \in C} (1 - m_{ab}^2)}$$

$C \in$ Generalized Loops = Loops without loose ends

$$m_{ab} = \int d\sigma_a b_a(\sigma_a) \sigma_{ab}$$

$$\mu_a = \int d\sigma_a b_a(\sigma_a) \prod_{b \in a, C} (\sigma_{ab} - m_{ab})$$

$b_{ab}, b_a, Z_0 \equiv -\ln F$ — all calculated within BP



- The Loop Series is finite
- BP is exact on a tree
- BP is a Gauge fixing condition.
Other choices of Gauges would lead to different representation.

• Replication:

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \sum_{\sigma'} \prod_a f_a(\sigma_a) \prod_{bc} \frac{1 + \sigma_{bc} \sigma_{cb}}{2}, \quad \sigma_{bc} \neq \sigma_{cb}$$

• Local Gauge Freedom:

$$1 + \pi\sigma = \frac{\exp(\sigma\eta + \pi\chi)}{\cosh(\eta + \chi)} \left(1 + (\tanh(\eta + \chi) - \sigma)(\tanh(\eta + \chi) - \pi) \cosh^2(\eta + \chi) \right)$$

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a \prod_{bc} V_{bc}, \quad P_a(\sigma_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

• Fixing the Gauge (η -fields on the graph)

BP equations

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) P_a(\sigma_a) = 0 \quad \Rightarrow \quad \eta_{j\alpha}^{bp} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{ij\beta}^{bp} \right)$$

Variational Principle:

Geometrical Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots *$$

$$\frac{\delta Z_0}{\delta \eta_{ab}} \Big|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta^{(bp)}}$$

• Replication:

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \sum_{\sigma'} \prod_a f_a(\sigma_a) \prod_{bc} \frac{1 + \sigma_{bc} \sigma_{cb}}{2}, \quad \sigma_{bc} \neq \sigma_{cb}$$

• Local Gauge Freedom:

$$1 + \pi\sigma = \frac{\exp(\sigma\eta + \pi\chi)}{\cosh(\eta + \chi)} \left(1 + (\tanh(\eta + \chi) - \sigma)(\tanh(\eta + \chi) - \pi) \cosh^2(\eta + \chi) \right)$$

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a \prod_{bc} V_{bc}, \quad P_a(\sigma_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

• Fixing the Gauge (η -fields on the graph)

BP equations

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) P_a(\sigma_a) = 0 \quad \Rightarrow \quad \eta_{j\alpha}^{bp} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{i\beta}^{bp} \right)$$

Variational Principle:

Geometrical Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots * \dots * \dots$$

$$\left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta^{(bp)}}$$

• Replication:

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \sum_{\sigma'} \prod_a f_a(\sigma_a) \prod_{bc} \frac{1 + \sigma_{bc} \sigma_{cb}}{2}, \quad \sigma_{bc} \neq \sigma_{cb}$$

• Local Gauge Freedom:

$$1 + \pi \sigma = \frac{\exp(\sigma \eta + \pi \chi)}{\cosh(\eta + \chi)} \left(1 + (\tanh(\eta + \chi) - \sigma)(\tanh(\eta + \chi) - \pi) \cosh^2(\eta + \chi) \right)$$

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a \prod_{bc} V_{bc}, \quad P_a(\sigma_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

• Fixing the Gauge (η -fields on the graph)

BP equations

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) P_a(\sigma_a) = 0 \quad \Rightarrow \quad \eta_{j\alpha}^{bp} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{i\beta}^{bp} \right)$$

Geometrical Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots *$$



Variational Principle:

$$\left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta^{(bp)}}$$

• Replication:

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \sum_{\sigma'} \prod_a f_a(\sigma_a) \prod_{bc} \frac{1 + \sigma_{bc} \sigma_{cb}}{2}, \quad \sigma_{bc} \neq \sigma_{cb}$$

• Local Gauge Freedom:

$$1 + \pi \sigma = \frac{\exp(\sigma \eta + \pi \chi)}{\cosh(\eta + \chi)} \left(1 + (\tanh(\eta + \chi) - \sigma)(\tanh(\eta + \chi) - \pi) \cosh^2(\eta + \chi) \right)$$

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a \prod_{bc} V_{bc}, \quad P_a(\sigma_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

• Fixing the Gauge (η -fields on the graph)

BP equations

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) P_a(\sigma_a) = 0 \quad \Rightarrow \quad \eta_{j\alpha}^{bp} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{i\beta}^{bp} \right)$$

Geometrical Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} *$$



Variational Principle:

$$\left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta^{(bp)}}$$

Pseudo-codewords Analysis: Merge results of Pseudo-Codeword-Search Algorithm & Loop Calculus

- Consider pseudo-codewords one after other
- For an individual pseudo-codeword/instanton identify a critical loop giving major contribution to the loop series:
 $Z = Z_0(1 + \sum_C r_C) \approx Z_0(1 + r(\Gamma))$
- Hint: look for single connected loops and use local "triad" contributions as a tester:

$$r(\Gamma) = \prod_{\alpha \in \Gamma} \tilde{\mu}_{\alpha}^{(bp)}, \quad \tilde{\mu}_{\alpha}^{(bp)} = \frac{\mu_{\alpha}^{(bp)}}{\sqrt{(1 - (m_i^{(bp)})^2)(1 - (m_j^{(bp)})^2)}}$$

Proof-of-Concept test [(155, 64, 20) code over AWGN]

- forall pseudo-codewords with $16.4037 < d < 20$ (~ 200 found)
there always exists a simple single-connected critical loop(s)
with $r(\Gamma) \sim 1$.
- Pseudo-codewords with the lowest d show $r(\Gamma) = 1$
- Invariant with respect to other choices of the original codeword
- Correction to log-likelihood at a bit of a critical loop brings the cumulative result to zero. Correction to an a-posteriori log-likelihood always aligns with correction to respective log-likelihood.

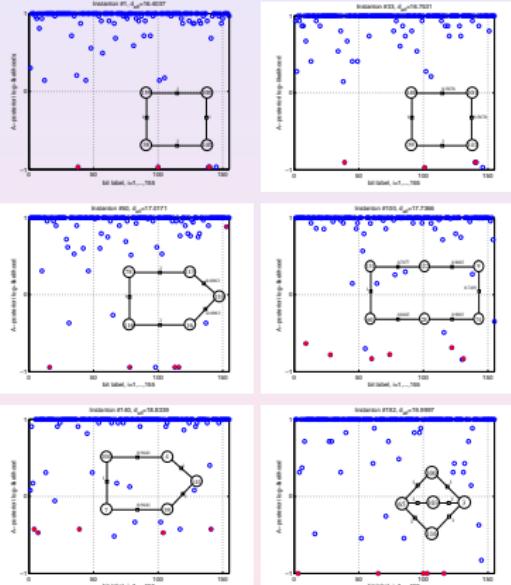
Pseudo-codewords Analysis: Merge results of Pseudo-Codeword-Search Algorithm & Loop Calculus

- Consider pseudo-codewords one after other
- For an individual pseudo-codeword/instanton identify a critical loop giving major contribution to the loop series:
 $Z = Z_0(1 + \sum_C r_C) \approx Z_0(1 + r(\Gamma))$
- Hint: look for single connected loops and use local "triad" contributions as a tester:

$$r(\Gamma) = \prod_{\alpha \in \Gamma} \tilde{\mu}_{\alpha}^{(bp)}, \quad \tilde{\mu}_{\alpha}^{(bp)} = \frac{\mu_{\alpha}^{(bp)}}{\sqrt{(1 - (m_i^{(bp)})^2)(1 - (m_j^{(bp)})^2)}}$$

Proof-of-Concept test [(155, 64, 20) code over AWGN]

- forall pseudo-codewords with $16.4037 < d < 20$ (~ 200 found) there always exists a simple single-connected critical loop(s) with $r(\Gamma) \sim 1$.
- Pseudo-codewords with the lowest d show $r(\Gamma) = 1$
- Invariant with respect to other choices of the original codeword
- Correction to log-likelihood at a bit of a critical loop brings the cumulative result to zero. Correction to an a-posteriori log-likelihood always aligns with correction to respective log-likelihood.



Bare BP Variational Principle:

$$\frac{\delta Z_0}{\delta \eta_{ab}} \Bigg|_{\eta(bp)} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Bigg|_{\eta(bp)}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \Bigg|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_\Gamma)$$

BP-equations are modified along the critical loop Γ

$$\frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \Bigg|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a' b') \in \Gamma} (1 - (m_{a' b'}^{(*)})^2)} \delta m_{a \rightarrow b; \Gamma} \Bigg|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

- 1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
- 2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_\Gamma|$. Triad search is helping.
- 3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
- 4. Return to Step 2 with an improved Γ -loop selection.



Bare BP Variational Principle:

$$\frac{\delta Z_0}{\delta \eta_{ab}} \Big|_{\eta(bp)} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta(bp)}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \Big|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_\Gamma)$$

BP-equations are modified along the critical loop Γ

$$\frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \Big|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a' b') \in \Gamma} (1 - \binom{*}{a' b'}^2)} \delta m_{a \rightarrow b; \Gamma} \Big|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

- 1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
- 2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_\Gamma|$. Triad search is helping.
- 3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
- 4. Return to Step 2 with an improved Γ -loop selection.



Bare BP Variational Principle:

$$\frac{\delta Z_0}{\delta \eta_{ab}} \Bigg|_{\eta_{(bp)}} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Bigg|_{\eta_{(bp)}}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \Bigg|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_\Gamma)$$

BP-equations are modified along the critical loop Γ

$$\frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \Bigg|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a'b') \in \Gamma} (1 - (m_{a'b'}^{(*)})^2)} \delta m_{a \rightarrow b;\Gamma} \Bigg|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

- 1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
- 2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_\Gamma|$. Triad search is helping.
- 3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
- 4. Return to Step 2 with an improved Γ -loop selection.



Bare BP Variational Principle:

$$\frac{\delta Z_0}{\delta \eta_{ab}} \Bigg|_{\eta_{(bp)}} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Bigg|_{\eta_{(bp)}}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \Bigg|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_\Gamma)$$

BP-equations are modified along the critical loop Γ

$$\frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \Bigg|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a' b') \in \Gamma} (1 - (m_{a' b'}^{(*)})^2)} \delta m_{a \rightarrow b; \Gamma} \Bigg|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

- 1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
- 2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_\Gamma|$. Triad search is helping.
- 3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
- 4. Return to Step 2 with an improved Γ -loop selection.



Even simpler algorithm

LP-erasure algorithm

1. Run LP algorithm. Terminate if LP succeeds (i.e. a valid code word is found).
2. If LP fails, find the most relevant loop Γ that corresponds to the maximal amplitude $r(\Gamma)$.
3. Modify the log-likelihoods along the loop Γ introducing a shift towards zero, i.e. introduce a complete or partial **erasure of the log-likelihoods at the bits**. Run LP with modified log-likelihoods. Terminate if the modified LP succeeds.
4. Return to **Step 2** with an improved selection principle for the critical loop.

(155, 64, 20) Test

IT WORKS!

All troublemakers (~ 200 of them) previously found by LP-based Pseudo-Codeword-Search Algorithm method were successfully **corrected** by the loop-improved LP algorithm.

- Method is invariant with respect the choice of the codeword (used to generate pseudo-codewords).

General Conjecture:

Loop-erasure algorithm is capable of reducing the error-floor.

Even simpler algorithm

LP-erasure algorithm

- 1. Run LP algorithm. Terminate if LP succeeds (i.e. a valid code word is found).
- 2. If LP fails, find the most relevant loop Γ that corresponds to the maximal amplitude $r(\Gamma)$.
- 3. Modify the log-likelihoods along the loop Γ introducing a shift towards zero, i.e. introduce a complete or partial **erasure of the log-likelihoods at the bits**. Run LP with modified log-likelihoods. Terminate if the modified LP succeeds.
- 4. Return to **Step 2** with an improved selection principle for the critical loop.

(155, 64, 20) Test

● IT WORKS!

All **troublemakers** (~ 200 of them) previously found by LP-based Pseudo-Codeword-Search Algorithm method were successfully **corrected** by the loop-improved LP algorithm.

- Method is invariant with respect the choice of the codeword (used to generate pseudo-codewords).

General Conjecture:

Loop-erasure algorithm is capable of reducing the error-floor.

Even simpler algorithm

LP-erasure algorithm

- 1. Run LP algorithm. Terminate if LP succeeds (i.e. a valid code word is found).
- 2. If LP fails, find the most relevant loop Γ that corresponds to the maximal amplitude $r(\Gamma)$.
- 3. Modify the log-likelihoods along the loop Γ introducing a shift towards zero, i.e. introduce a complete or partial **erasure of the log-likelihoods at the bits**. Run LP with modified log-likelihoods. Terminate if the modified LP succeeds.
- 4. Return to **Step 2** with an improved selection principle for the critical loop.

(155, 64, 20) Test

● IT WORKS!

All **troublemakers** (~ 200 of them) previously found by LP-based Pseudo-Codeword-Search Algorithm method were successfully **corrected** by the loop-improved LP algorithm.

- Method is invariant with respect the choice of the codeword (used to generate pseudo-codewords).

General Conjecture:

Loop-erasure algorithm is capable of reducing the error-floor.

Results

- Loop Calculus
 - = Generic Tool for calculating marginal probabilities in terms of loops on underlying graphical structure
- Pseudo-Codeword-Search Algorithm
 - = Efficient way of describing pseudo-codeword spectrum for LP-decoding
- Pseudo-Codewords are all associated with respective Critical Loops
- Effective Free Energy Approach
 - = Variational Principle improving BP with a Critical Loop information
- Loop-corrected BP and Loop-erasure
 - = Algorithms improving BP/LP with a Critical Loop information

Future Efforts

- Improve and continue testing the simple LP-erasure algorithm.
- The major improvement required is in automatization of the critical loop identification scheme. (Towards Monte Carlo test.)
- Testing other (longer) codes.
- Testing other (e.g. correlated) channels.
- All of the above for improving Loop-corrected BP.

Other complementary developments, e.g. on

- Improving LP [Dimakis, Wainwright '06]
- Reducing LP complexity [Taghavi, Siegel '06; Vontobel, Koetter '06]
- Accelerating convergence of bare BP [Stepanov, Chertkov '06]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]

Bibliography

- M. Chertkov, V.Y. Chernyak, *Loop Calculus Helps to Improve Belief Propagation and Linear Programming Decodings of Low-Density-Parity-Check Codes*, 44th Allerton Conference (September 27-29, 2006, Allerton, IL)
- M. Chertkov, V.Y. Chernyak, *Loop Calculus in Statistical Physics and Information Science*, Phys. Rev. E **73**, 065102(R) (2006); cond-mat/0601487.
- M. Chertkov, V.Y. Chernyak, *Loop series for discrete statistical models on graphs*, J. Stat. Mech. (2006) P06009, cond-mat/0603189.
- M. Chertkov, M.G. Stepanov, *An Efficient Pseudo-Codeword Search Algorithm for Linear Programming Decoding of LDPC Codes*, arXiv:cs.IT/0601113, submitted to IEEE Transactions on Information Theory.
- M.G. Stepanov, V. Chernyak, M. Chertkov, B. Vasic, *Diagnosis of weakness in error correction: a physics approach to error floor analysis*, Phys. Rev. Lett. **95**, 228701 (2005) [See also <http://www.arxiv.org/cond-mat/0506037> for extended version with Supplements.]
- M.G. Stepanov, M. Chertkov, *Instanton analysis of Low-Density-Parity-Check codes in the error-floor regime*, arXiv:cs.IT/0601070, ISIT 2006 (July 2006, Seattle, WA)
- M.G. Stepanov, M. Chertkov, *Improving convergence of belief propagation decoding*, arXiv:cs.IT/0607112, 44th Allerton Conference (September 27-29, 2006, Allerton, IL)